WHAT IS CLAIMED IS:

1. A transaction authorization system for authorizing a transaction requested by an authorized user while preventing authorization of a transaction requested by an unauthorized user, comprising:

(a) a user device which comprises:

(i) an identity verification unit operable to receive current biometric input from a current user, and to utilize said current biometric input to determine if said current user is an authorized user of said user device;

(ii) a transaction code provider operable to provide a transaction code if, and only if, said identity verification unit determines that a current user is an authorized user of said user device; and

(iii) a first communication device operable to communicate said transaction code; and

(b) a server device which comprises:

(i) a second communication device operable to receive a communicated code;

(ii) a transaction code verifier operable to determine if said received communicated code is a transaction code provided by said transaction code provider; and

(iii) an authorizer operable to authorize a transaction if and only if said transaction code verifier determines that said received communicated code is a transaction code provided by said transaction code provider.

2. The system of claim 1, further comprising a system for executing a business transaction authorized by said authorizer.

3. The system of claim 1, wherein said user device is formed in a size and shape substantially similar to a credit card.

4. The system of claim 1, wherein said user device is a smart card.

5. The system of claim 1, wherein said user device conforms to ISO standard 7816.

6. The system of claim 1, wherein said user device includes a battery.

7. The system of claim 6, wherein said battery is a replaceable battery.

8. The system of claim 6, wherein said battery is a rechargeable battery.

9. The system of claim 1, wherein said user devices comprises a photocell operable to supply power to said user device.

10. The system of claim 1, wherein said identity verification unit comprises a biometric sensor.

11. The system of claim 10, wherein said biometric sensor comprises a fingerprint sensor.

12. The system of claim 11, wherein said fingerprint sensor comprises an optical sensor.

13. The system of claim 11, wherein said fingerprint sensor comprises a capacitance sensor.

14. The system of claim 10, wherein said biometric sensor comprises a microphone.

15. The system of claim 10, wherein said biometric sensor comprises a sound recording device.

16. The system of claim 10, wherein said biometric sensor comprises a digital camera.

17. The system of claim 10, wherein said biometric sensor comprises a voice recognition system.

18. The system of claim 10, wherein said biometric sensor comprises a retinal pattern scanner.

19. The system of claim 10, wherein said biometric sensor comprises a signature verification system.

20. The system of claim 10, wherein said biometric sensor comprises an iris scanning module.

21. The system of claim 10, wherein said biometric sensor comprises a module operable to measure part of a body of a user.

22. The system of claim 21, wherein said biometric sensor comprises a module operable to measure features of a hand of a user.

09976044 .101501

23. The system of claim 21, wherein said biometric sensor comprises a module operable to measure features of a face of a user.

24. The system of claim 10, wherein said biometric sensor comprises a module operable to measure a movement of a user.

25. The system of claim 10, wherein said biometric sensor comprises a module operable to measure a behavior of a user.

26. The system of claim 10, wherein said biometric sensor comprises a module operable to characterize a pattern of physical interaction between said biometric sensor and a user.

27. The system of claim 10, wherein said identity verification unit further comprises a first data memory operable to store biometric data of an authorized user.

28. The system of claim 27, further comprising biometric data of an authorized user stored in said first data memory.

29. The system of claim 28, wherein said biometric data of an authorized user is a calculated data resulting from a calculation based on at least one sample of input from a biometric sensor operated by a user identified as an authorized user of said user device.

30. The system of claim 27, wherein said identity verification unit further comprises a first processor operable to compare biometric data of an authorized user stored in said first data memory to current biometric data sensed by said biometric sensor.

09976044.101501

31. The system of claim 30, wherein said first processor is further operable to determine that said current user of said user device is an authorized user of said user device whenever detected differences between said biometric data of an authorized user and said current biometric data of a current user are less than a predetermined amount of difference.

32. The system of claim 1, wherein said first communication device of said user device comprises a graphical display module operable to optically display a transaction code provided by said transaction code provider.

33. The system of claim 32, wherein said graphical display module comprises an LCD.

34. The system of claim 32, wherein said graphical display module comprises a light-emitting element.

35. The system of claim 34, wherein said light-emitting element comprises an organic compound operable to emit light when electrically powered.

36. The system of claim 32, wherein said graphics display module comprises a plasma display.

37. The system of claim 32, wherein said graphical display module is operable to display said transaction code in a machine-readable format.

38. The system of claim 37, wherein said graphical display module is operable to display said transaction code in barcode format.

10057047.101501

39. The system of claim 37, wherein said graphical display module is operable to display said transaction code in a format readable by an optical character recognition system.

40. The system of claim 32, wherein said graphical display module is operable to display said transaction code in a format readable by a human user and also readable by an optical character recognition system.

41. The system of claim 32, wherein said graphical display module is operable to display said transaction code in a format readable by a human user.

42. The system of claim 1 wherein said first communication device comprises a machine readable memory, and further comprises electrical connections operable to enable reading of said machine readable memory by a processor external to said user device.

43. The system of claim 1, wherein said first communication device comprises a transmitter.

44. The system of claim 43, wherein said transmitter comprises an emitter of radio frequencies.

45. The system of claim 43, wherein said transmitter comprises an emitter of optical frequencies.

46. The system of claim 43, wherein said transmitter comprises an emitter of infrared frequencies.

47. The system of claim 43, wherein said transmitter is operable to transmit said transaction code to a receiver, said receiver being operable to

transmit said transaction code to said second communication device of said server device.

48. The system of claim 43, wherein said transmitter comprises a sound generator.

49. The system of claim 48, wherein said sound generator is operable to generate frequencies audible to the human ear.

50. The system of claim 48, wherein said sound generator is operable to generate frequencies inaudible to the human ear.

51. The system of claim 1, wherein said first communication device is operable to communicate said transaction code during a limited lapse of time, and to cease communicating said transaction code at expiration of said lapse of time.

52. The system of claim 51, wherein said lapse of time is less than two minutes duration.

53. The system of claim 51, wherein said lapse of time is approximately 30 seconds.

54. The system of claim 1, wherein said transaction code provider comprises a first code memory operable to store a set of substantially random digital codes.

55. The system of claim 54, wherein said transaction code provider further comprises a selector operable to select a next transaction code from among codes stored in said first code memory.

56. The system of claim 55, further comprising a first disqualifier for disqualifying a code stored in said first code memory from future selection by said selector.

57. The system of claim 55, further comprising a first disqualifier operable to remove a transaction code from said first code memory, thereby preventing its future selection by said selector.

58. The system of claim 1, wherein said transaction code provider is operable to provide a non-predictable transaction code.

59. The system of claim 58, wherein said transaction code provider is designed and constructed to refrain from providing a transaction code previously provided by said transaction code provider.

60. The system of claim 1, wherein said transaction code verifier comprises a second code memory operable to store a set of substantially random digital codes.

61. The system of claim 60, further comprising a set of substantially random digital codes stored in said second code memory.

62. The system of claim 1, wherein said user device comprises a first code memory storing a first set of substantially random digital codes, and said server device comprises a second code memory storing a second set of substantially random digital codes, said first set of substantially random digital codes and said second set of substantially random digital codes being identical.

63. The system of claim 1, wherein said user device comprises a first code memory storing a first set of substantially random digital codes, and said server device comprises a second code memory storing a second set of substantially random digital codes, said first set of substantially random digital codes and said second set of substantially random digital codes being substantially similar.

64. The system of claim 63, wherein said transaction code verifier comprises a code tester for testing a received code to determine if said received code is a transaction code provided by said user device.

65. The system of claim 64, wherein said code tester comprises a code searcher operable to compare said received code to said codes stored in said second code memory to determine if said received code is identical to a code stored in said second code memory.

66. The system of claim 65, wherein said authorizer is operable to authorize a transaction if and only if said received code is determined to be identical to a code stored in said second code memory.

67. The system of claim 65, further comprising a second disqualifier operable to disqualify a selected code stored in said second code memory when said selected code is found by said code searcher to be identical to said received code, said disqualification preventing said disqualified code from being examined by said code searcher during subsequent searches of said codes stored in said second code memory by said code searcher.

68. The system of claim 65, further comprising a second disqualifier operable to remove from said second code memory a selected code stored in

said second code memory when said selected code has been found to be identical to said received code.

69. The system of claim 1, wherein said transaction code provider comprises an first algorithmic pseudo-random code generator operable to generate a transaction code.

70. The system of claim 69, wherein said transaction code tester comprises a second algorithmic pseudo-random code generator operable to generate a set of generated codes, said transaction code tester being further operable to compare said received code to each generated code of said set of generated codes.

71. The system of claim 69, wherein said authorizer is operable to authorize a transaction if and only if said received code is found to be identical to a generated code belonging to said set of generated codes.

72. The system of claim 1, wherein said user device comprises a portable device and a stationary device.

73. The system of claim 72, wherein said portable device is formed in a size and shape substantially similar to a credit card, and said stationary devices comprises a biometric sensor.

74. The system of claim 73, wherein said portable devices comprises a memory operable to store biometric data of an authorized user.

75. A user-identifying device operable to identify an authorized user of said device, comprising:

10054752.101501

(a) a memory for storing biometric data of an authorized user of said device;

(b) a biometric sensor operable to receive current biometric data of a current user of said device;

(c) a processor operable to compare said current biometric data of said current user to said stored biometric data of said authorized user; and

(d) a communicator operable to communicate information, said information being communicated only if said processor determines that said current biometric data is similar to said stored biometric data.

76. The device of claim 75, further comprising a transaction code provider operable to provide a non-predictable transaction code useable to provoke authorization of a business transaction by a transaction authorizing authority, said transaction code being provided by said transaction code provider and communicated by said communicator only if said processor determines that said current biometric data is similar to said stored biometric data.

77. The device of claim 75, wherein said device is formed in a size and shape substantially similar to a credit card.

78. The device of claim 75, wherein said device is a smart card.

79. The device of claim 75, wherein said device conforms to ISO standard 7816.

80. The device of claim 75, further comprising a battery.

81. The device of claim 80, wherein said battery is a replaceable battery.

82. The device of claim 80, wherein said battery is a rechargeable battery.

83. The device of claim 75, further comprising a photocell operable to supply power to said device.

84. The device of claim 75, wherein said biometric sensor comprises a fingerprint sensor.

85. The device of claim 84, wherein said fingerprint sensor comprises an optical sensor.

86. The device of claim 84, wherein said fingerprint sensor comprises a capacitance sensor.

87. The device of claim 75, wherein said biometric sensor comprises a microphone.

88. The device of claim 75, wherein said biometric sensor comprises a sound recording device.

89. The device of claim 75, wherein said biometric sensor comprises a digital camera.

90. The device of claim 75, wherein said biometric sensor comprises a voice recognition system.

10037045.101502

91. The device of claim 75, wherein said biometric sensor comprises a retinal pattern scanner.

92. The device of claim 75, wherein said biometric sensor comprises a signature verification system.

93. The device of claim 75, wherein said biometric sensor comprises an iris scanning module.

94. The device of claim 75, wherein said biometric sensor comprises a module operable to measure part of a body of a user.

95. The device of claim 75, wherein said biometric sensor comprises a module operable to measure features of a hand of a user.

96. The device of claim 75, wherein said biometric sensor comprises a module operable to measure features of a face of a user.

97. The device of claim 75, wherein said biometric sensor comprises a module operable to measure a movement of a user.

98. The device of claim 75, wherein said biometric sensor comprises a module operable to measure a behavior of a user.

99. The device of claim 75, wherein said biometric sensor comprises a module operable to characterize a pattern of physical interaction between said biometric sensor and a user.

100. The device of claim 75, further comprising biometric data of an authorized user stored in said memory.

101. The device of claim 100, wherein said biometric data of an authorized user is a calculated data resulting from a calculation based on at least one sample of input from a biometric sensor operated by a user identified as an authorized user of said device.

102. The device of claim 75, wherein said processor is operable to determine that a current user of said device is an authorized user of said device whenever detected differences between said biometric data of an authorized user and said current biometric data of a current user are less than a predetermined amount of difference.

103. The device of claim 75, wherein said communication device comprises a graphical display module operable to optically display information.

104. The device of claim 76, wherein said graphical display module is operable to optically display a transaction code provided by said transaction code provider.

105. The device of claim 103, wherein said graphical display module comprises an LCD.

106. The device of claim 103, wherein said graphical display module comprises a light-emitting element.

107. The device of claim 106, wherein said light-emitting element comprises an organic compound operable to emit light when electrically powered.

108. The device of claim 103, wherein said graphics display module comprises a plasma display.

109. The device of claim 104, wherein said graphical display module is operable to display said transaction code in a machine-readable format.

110. The device of claim 109, wherein said graphical display module is operable to display said transaction code in barcode format.

111. The device of claim 109, wherein said graphical display module is operable to display said transaction code in a format readable by an optical character recognition system.

112. The device of claim 104, wherein said graphical display module is operable to display said transaction code in a format readable by a human user and also readable by an optical character recognition system.

113. The device of claim 103, wherein said graphical display module is operable to display said information in a format readable by a human user.

114. The device of claim 103, wherein said graphical display module is operable to display said information in a machine-readable format.

115. The device of claim 114, wherein said graphical display module is operable to display said information in barcode format.

116. The device of claim 104, wherein said graphical display module is operable to display said transaction code in a format readable by a human user.

117. The device of claim 75 wherein said communication device comprises a machine readable memory, and further comprises electrical

connections operable to enable reading of said machine readable memory by a processor external to said device.

118. The device of claim 75, wherein said communication device comprises a transmitter.

119. The device of claim 118, wherein said transmitter comprises an emitter of radio frequencies.

120. The device of claim 118, wherein said transmitter comprises an emitter of optical frequencies.

121. The device of claim 118, wherein said transmitter comprises an emitter of infrared frequencies.

122. The device of claim 118, wherein said transmitter comprises a sound generator.

123. The device of claim 122, wherein said sound generator is operable to generate frequencies audible to the human ear.

124. The device of claim 122, wherein said sound generator is operable to generate frequencies inaudible to the human ear.

125. The device of claim 75, wherein said communication device is operable to communicate said information during a limited lapse of time, and to cease communicating said information at expiration of said lapse of time.

126. The device of claim 125, wherein said lapse of time is less than two minutes duration.

127. The device of claim 125, wherein said lapse of time is approximately 30 seconds.

128. The device of claim 76, wherein said transaction code provider comprises a first code memory operable to store a set of substantially random digital codes.

129. The device of claim 128, wherein said transaction code provider further comprises a selector operable to select a next transaction code from among codes stored in said first code memory.

130. The device of claim 129, further comprising a first disqualifier for disqualifying a code stored in said first code memory from future selection by said selector.

131. The device of claim 129, further comprising a first disqualifier operable to remove a transaction code from said first code memory, thereby preventing its future selection by said selector.

132. The device of claim 76, wherein said transaction code provider is designed and constructed to refrain from providing a transaction code previously provided by said transaction code provider.

133. A server device operable to authorize a transaction, the device comprising:

(a) a communication device operable to receive a communicated transaction request and an associated communicated code;

(b) a transaction code verifier operable to determine if said received communicated code is a valid transaction code provided by a user-identifying device; and

(c) an authorizer operable to authorize a transaction if and only if said transaction code verifier determines that said received communicated code is a transaction code provided by said a user-identifying device.

134. The device of claim 133, wherein said transaction code verifier comprises a code memory operable to store a set of substantially random digital codes.

135. The device of claim 134, further comprising a set of substantially random digital codes stored in said code memory.

136. The device of claim 133, wherein said transaction code verifier comprises a code tester for testing a received code to determine if said received code is a valid transaction code provided by a user-identifying device.

137. The device of claim 136, wherein said code tester comprises a code searcher operable to compare said received code to said codes stored in said code memory to determine if said received code is identical to a code stored in said code memory.

138. The device of claim 137, wherein said authorizer is operable to authorize a transaction if and only if said received code is determined to be identical to a code stored in said code memory.

139. The device of claim 137, further comprising a disqualifier operable to disqualify a selected code stored in said code memory when said selected code is found by said code searcher to be identical to said received code, said disqualification preventing said disqualified code from being

examined by said code searcher during subsequent searches of said codes stored in said code memory by said code searcher.

140. The device of claim 137, further comprising a disqualifier operable to remove from said code memory a selected code stored in said code memory when said selected code has been found to be identical to said received code.

141. The device of claim 75, wherein said transaction code provider comprises an first algorithmic pseudo-random code generator operable to generate a transaction code.

142. The device of claim 141, wherein said transaction code tester comprises a second algorithmic pseudo-random code generator operable to generate a set of generated codes, said transaction code tester being further operable to compare said received code to each generated code of said set of generated codes.

143. The device of claim 141, wherein said authorizer is operable to authorize a transaction if and only if said received code is found to be identical to a generated code belonging to said set of generated codes.

144. The device of claim 75, further comprising a portable device and a stationary device.

145. The device of claim 144, wherein said portable device is formed in a size and shape substantially similar to a credit card, and said stationary device comprises a biometric sensor.

146. The device of claim 145, wherein said portable devices comprises a memory operable to store biometric data of an authorized user.

147. A user-identifying device providing a non-predictable transaction code useable to authenticate a business transaction, comprising:

(a) a memory for storing biometric data of an authorized user of said device;

(b) a biometric sensor operable to receive current biometric data of a current user of said device;

(c) a biometric data comparator for comparing said current biometric data of said current user to said stored biometric data of said authorized user; and

(d) a transaction code generator operable to generate a non-predictable transaction code useable to provoke authorization of a business transaction by a transaction authorizing authority, said transaction code being generated only if said biometric data comparator determines that said current biometric data is similar to said stored biometric data.

148. A method for authorizing a transaction requested by an authorized user of a transaction authorizing system and for preventing authorization of a transaction requested by an unauthorized user of said transaction authorizing system, the method comprising:

(a) utilizing a user device to:

(i) receive biometric data from a current user;

(ii) compare said received biometric data from a current user to stored biometric data from an authorized user, to determine if they are similar; and

(iii) provide and communicate a non-predictable transaction code if and only if said stored biometric data from an authorized user and said received biometric data from a current user are determined to be similar; and

(b) utilizing a server device to:

(i) receive a communicated transaction request accompanied by a communicated code;

(ii) determine whether said received communicated code is a transaction code provided by said user device;

(iii) authorize said transaction if and only if said received communicated code is determined to be a transaction code provided by said user device,

thereby enabling authorization of a transaction requested by an authorized user, and preventing authorization of a transaction requested by an unauthorized user.

149. The method of claim 148, further comprising executing a business transaction authorized by said authorizer.

150. The method of claim 148, wherein receiving biometric data from a current user includes receiving fingerprint data from said current user.

151. The method of claim 148, wherein receiving biometric data from a current user includes receiving sound data from said current user.

152. The method of claim 148, wherein receiving biometric data from a current user includes receiving voice data from said current user.

153. The method of claim 148, wherein receiving biometric data from a current user includes receiving optical data from said current user.

09976044.101501

154. The method of claim 148, wherein receiving biometric data from a current user includes receiving data generated by said current user writing a signature.

155. The method of claim 148, wherein receiving biometric data from a current user includes receiving a retinal pattern of said current user.

156. The method of claim 148, wherein receiving biometric data from a current user includes receiving a iris pattern of said current user.

157. The method of claim 148, wherein receiving biometric data from a current user includes measuring a part of a body of said current user.

158. The method of claim 157, wherein measuring a part of a body of a user includes measuring a feature of a hand of said current user.

159. The method of claim 157, wherein measuring a part of a body of a user includes measuring a feature of a face of said current user.

160. The method of claim 148, wherein receiving biometric data from a current user includes measuring a movement of said current user.

161. The method of claim 148, wherein receiving biometric data from a current user includes measuring a behavior of said current user.

162. The method of claim 148, wherein receiving biometric data from a current user includes measuring a pattern of physical interaction between said user device and said current user.

163. The method of claim 148, wherein comparing said received biometric data from a current user to said stored biometric data from an authorized user includes determining whether detected differences between said stored biometric data of an authorized user and said received biometric data of a current user are less than a predetermined amount of difference.

164. The method of claim 148, wherein communicating said non-predictable transaction code includes displaying said transaction code on a graphical display module.

165. The method of claim 148, wherein communicating said non-predictable transaction code includes displaying said transaction code in a machine-readable format.

166. The method of claim 148, wherein communicating said non-predictable transaction code includes displaying said transaction code in a barcode format.

167. The method of claim 148, wherein communicating said non-predictable transaction code includes displaying said transaction code in a format readable by an optical character recognition system.

168. The method of claim 148, wherein communicating said non-predictable transaction code includes displaying said transaction code in a format readable by a human user.

169. The method of claim 148, wherein communicating said non-predictable transaction code includes utilizing a processor external to said user device to read a machine readable memory of said user device.

09976044.101501

170. The method of claim 148, further comprising receiving communication of a transaction code from said user device and communicating said transaction code to said server device.

171. The method of claim 148, further comprising limiting a duration of said communication of said transaction code to a period of less than two minutes.

172. The method of claim 148, further comprising limiting a duration of said communication of said transaction code to a period of approximately 30 seconds.

173. The method of claim 148, further including providing said transaction code by selecting said transaction code from among a set of substantially random digital codes stored in a memory of said user device.

174. The method of claim 148, further including verifying said received code by determining if said received code is identical to a code stored in a memory of said server device.

175. The method of claim 148, further including providing said transaction code by utilizing a processor of said user device to generate said transaction code by utilizing a pseudo-random code generation algorithm.